REMARKS

The Office Action dated January 10, 2008 has been carefully reviewed and the foregoing amendment has been made in consequence thereof.

Claims 1-25, 27, 28, 30-56, 58, 60-74, 76-89, and 119-122 are now pending in this application. Claims 1-25, 27, 28, 30-56, 58, 60-89, and 119-122 stand rejected. Claim 75 has been canceled.

The rejection of Claims 1-25, 27, 28, 30-56, 58, 60-89, and 119-122 under 35 U.S.C. § 101 as being directed to non-statutory subject matter is respectfully traversed.

The Office Action asserts that Claims 1-25, 27, 28, 30-56, 58, 60-89, and 119-122 are directed to non-statutory subject matter because, in the present case, "the result of the invention is not considered to be concrete (i.e., it is not capable of being repeated to arrive at a particular result) . . ." and "because the results are not concrete, the examiner does not see how the result is useful…."

Specifically, the Office Action assets that Claims 1, 16-18, 24, 31, 63, and 76 are directed to non-statutory subject matter because "[t]he examiner takes notice of the fact that it is a person that decides what values the variable of 'detection rating,' 'severity rating,' and 'process strength rating' are supposed to have." Moreover, the Office Action asserts that "[b]ecause all of the variables used to calculate the QFD score are disclosed as being determined by people and because there is no guidance given on how to go about choosing the appropriate values for these variables, the result of the invention is not considered to be concrete…." The Office Action further asserts that "[b]ecause of the fact that different people may ascribe different values to the variables used in the equation, and because no guidance is given on how to go about choosing the values for the 'detection rating,' 'severity rating,' and 'process strength rating,' the result is not guaranteed. The claim is not statutory because the result is not concrete (i.e. it is not capable of being repeated due to the human factor)."

Applicants traverse these assertions. First, Applicants respectfully submit that the mere fact that certain variables used to calculate an output may be measured by a person, such as an experienced risk assessor, does not mean that the output is non-repeatable or that the invention fails to produce a concrete result. In fact, such a system does produce a concrete and repeatable result that is directly based on the information inputted into the system.

Secondly, with respect to the present application, Applicants submit that those variables are not solely determined by a person without guidance. Rather, the originally filed specification clearly describes these variables being determined based on information included in a knowledge base and/or known rating systems, wherein the known rating system is defined within the knowledge base. For example, the originally filed specification provides the following:

> In one embodiment, server 12 is configured to use the knowledge base to determine what constitutes an affirmative answer to a question in the questionnaire. Compliance is largely dependent upon the particular circumstances of each business. Accordingly, *the knowledge base may include, for example, information from compliance leaders and information relevant to each business and for each environment. The knowledge base may also include standards for minimum program qualities and the level of documentation required* for proof in answering the question which sets a standard used as a guide through the interviews with process owners. (Paragraph [0058]). (Emphasis added).
>
> Subsequently, a list of compliance requirements is compiled and prioritized by the resource team. The list of compliance requirements is compiled and prioritized by using and adding to database 18 stored on server 12 (shown in Figures 1 and 2). Database 18 includes, for example, the core compliance areas within the business' declared policies and procedures (referred to as the business Spirit and Letter), regulatory and legal requirements of the business, contractual and internal policy requirements, and compliance risks noted in business risk model 160 (shown in Figure 10). As described above, the list of compliance requirements also is prioritized. In an exemplary embodiment, the list of compliance requirements is prioritized by the resource team based on the severity rating of non-compliance. *Severity ratings are generated using stored and newly added knowledge base information relevant to severity. The knowledge base includes information relating to how a compliance expert, in a worst case*

scenario situation, would rate damage to the business reputation and/or the financial impact to a business. The knowledge base may be specific to individual business processes and products. For example, when a business reputation is damaged, the severity rating of non-compliance is high when it has a company impact, medium when it has a division impact and low when it has only a regional impact. The list of compliance requirements is organized in accordance with a severity matrix format. *Accordingly, in one specific embodiment, the financial impact of non-compliance is rated high when there is an impact greater than ten percent of net income, medium when the impact is greater than five percent, but less than ten percent, of net income, and low when it has an impact affecting less than five percent of net income.* Alternatively, different weighting formulas can be used. (Paragraph [0072]). (Emphasis added).

Further, the process strength of a business routines and controls is assessed to ensure compliance with each policy. In one specific embodiment, the assessment is accomplished by rating, or quantifying, the strength of the compliance routines and controls to ensure compliance with the policy. *The process strength rating may be accomplished by any known rating system. In one specific embodiment, a score of ten means that there is no process or no level of policy awareness. A score of seven indicates an inconsistent process, no documentation or sporadic, ad hoc generic training. A score of three means that there is no enforced process, limited enforced process or no regular specific training. A score of zero means that there is no interaction or no process is necessary.* This score is used to calculate a QFD score for quantifying the results. (Paragraph [0076]). (Emphasis added).

Also, issues relating to risk are identified, for example, determination of potential failures and root causes of the failures. The cross functional resource team is reassembled in order to execute extensive failure mode and effects analysis (FMEA) on the top three to five compliance requirements risks identified in the RPM above. Referring to Figure 14, a flowchart 200 illustrating process steps executed in addressing the top three to five compliance requirements risks identified in the RPM is shown. After mapping 202 steps for each risk, for example by giving each process step in the risk a name that clearly identifies the step, the risks are analyzed by the team to determine 204 potential failure modes. The effect of each failure mode is determined 206 by the team who then try to identify 208 the potential causes of each failure mode. The high-risk process steps are mapped 202 and a failure mode and effects analysis matrix (FMEA) is constructed. *In constructing the FMEA a severity rating, current controls in place are listed 210, a likelihood of occurrence factor and*

> *a detection ability factor is assigned 212 based on a standard rating system which is part of the knowledge base in server 12. Server 12 is configured to use the rating system and the entered factors to calculate 214 risk prioritization numbers (RPNs).* Next, recommended actions to reduce RPNs are determined 216 by the team. Specifically, and in one embodiment, a RPN enables the team to prioritize actions for implementation and allocate resources effectively to reduce the RPN. In a specific embodiment, progress in reducing an RPN is monitored and team actions are guided by system 10 using the knowledge base stored within server 12. (Paragraph [0081]). (Emphasis added).

Accordingly, Applicants have shown that the variables used to calculate the QFD are based on information included in a knowledge base and/or known rating systems. The specification does not describe or suggest that the variables are assigned values <u>based on personal knowledge of the team members</u> as asserted in the Office Action. Rather, as shown above, the method describes that preferably a value is assigned to the detection rating, severity rating, and process strength rating using information included in the knowledge base, known rating systems, and/or predetermined variable values. As such, the result produced by the method is repeatable and thus concrete.

For at least the reasons set forth above, Applicants respectfully request that the Section 101 rejection of Claims 1-25, 27, 28, 30-56, 58, 60-89, and 119-122 be withdrawn.

The rejection of Claims 1-25, 27, 28, 30-56, 58, 60-89, and 119-122 under 35 U.S.C. § 112, first paragraph, as failing to comply with the enablement requirement is respectfully traversed.

Applicants respectfully submit that the specification meets the requirements of Section 112, first paragraph. Specifically, Applicants respectfully submit that the specification, including the figures, would enable one skilled in the art to make and/or use the invention as described in the present patent application. Accordingly, Applicants respectfully request that the rejection of Claims 1-25, 27, 28, 30-56, 58, 60-89, and 119-122 under Section 112, first paragraph, be withdrawn.

With respect to Claim 1, Claim 1 recites in part a step of "identifying, for each compliance risk identified, potential compliance failure modes, potential causes and effects of such compliance failure modes, current controls in place, and a detection rating, wherein the detection rating is a value representing whether current controls in place will detect potential compliance failure modes...." The Office Action asserts that "it is a person that decides what value the variables of 'detection rating' is supposed to have" and that "the specification provides no guidance on how one should go about determining the correct values for this variable . . . without undue experimentation (which is present due to the lack of guidance)."

Applicants respectfully traverse this assertion. For the same reasons set forth above, Applicants respectfully submit that the originally filed specification provides support for the recitations included in the present claims. Specifically, Applicants submit that the recitation that provides "the detection rating is a value representing whether current controls in place will detect potential compliance failure modes" is fully supported by the originally filed specification and, therefore, is enabling. For example, the specification provides the following:

> In one embodiment, server 12 is configured to use the knowledge base to determine what constitutes an affirmative answer to a question in the questionnaire. Compliance is largely dependent upon the particular circumstances of each business. Accordingly, *the knowledge base may include, for example, information from compliance leaders and information relevant to each business and for each environment. The knowledge base may also include standards for minimum program qualities and the level of documentation required* for proof in answering the question which sets a standard used as a guide through the interviews with process owners. (Paragraph [0058]). (Emphasis added).
>
> Also, issues relating to risk are identified, for example, determination of potential failures and root causes of the failures. The cross functional resource team is reassembled in order to execute extensive failure mode and effects analysis (FMEA) on the top three to five compliance requirements risks identified in the RPM above. Referring to Figure 14, a flowchart 200 illustrating process steps executed in addressing the top three to five compliance requirements risks identified in the RPM is shown. After mapping 202 steps for each risk, for example by giving each process step in the risk a name that clearly identifies the step, the risks are analyzed by the team to determine 204 potential failure modes. The effect of each failure mode is determined 206 by the team who then try to identify 208 the

> potential causes of each failure mode. The high-risk process steps are mapped 202 and a failure mode and effects analysis matrix (FMEA) is constructed. *In constructing the FMEA a severity rating, current controls in place are listed 210, a likelihood of occurrence factor and a detection ability factor is assigned 212 based on a standard rating system which is part of the knowledge base in server 12. Server 12 is configured to use the rating system and the entered factors to calculate 214 risk prioritization numbers (RPNs).* Next, recommended actions to reduce RPNs are determined 216 by the team. Specifically, and in one embodiment, a RPN enables the team to prioritize actions for implementation and allocate resources effectively to reduce the RPN. In a specific embodiment, progress in reducing an RPN is monitored and team actions are guided by system 10 using the knowledge base stored within server 12. (Paragraph [0081]). (Emphasis added).

As such, the specification describes a method for conducting a consistent, documented, and repeatable compliance risk assessment and mitigation process in which potential compliance failure modes, potential causes and effect of the compliance failure modes, current controls in place, and a detection rating are each identified for a number of identified compliance risks. As such, Applicants respectfully traverse the assertion in the Office Action that the specification describes that people determine what the detection rating value is without also describing on what information the detection rating is based. Specifically, Applicants describe that the detection rating is based on a standard or known rating system that is included in a knowledge base. Applicants describe the knowledge base as including, for example, information from compliance leaders, information relevant to each business and for each environment, and standards for minimum program qualities and the level of documentation required. As such, Applicants describe that the detection rating is based on readily available information, rather than on subjective estimates and/or choices. Accordingly, Applicants submit that the recitations of Claim 1 are supported and clearly described in the originally filed specification.

Claim 31 recites a system that includes a server configured to perform steps substantially identical to those described with regards to Claim 1 above. As such, the recitations of Claim 31 are likewise submitted to be supported in the originally filed specification.

Claim 63 recites a computer that is configured to perform steps substantially identical to those described with regards to Claim 1 above. As such, the recitations of Claim 63 are likewise submitted to be supported in the originally filed specification.

Claim 76 recites a computer program that includes at least one code segment for performing steps substantially identical to those described with regards to Claim 1 above. As such, the recitations of Claim 76 are likewise submitted to be supported in the originally filed specification.

With regards to Claim 31, the Office Action asserts that "one of skill in the art would not be able to make the server do what is claimed." More specifically, the Office Action asserts that the specification does not describe how the server is programmed in order to prioritize compliance risks for a business, identify potential failure modes with causes and effects, and recommend risk monitoring and control mechanisms without requiring undue experimentation.

Applicants respectfully traverse these assertions. Specifically, the server includes a knowledge base that, as discussed above, includes, for example, "information from compliance leaders and information relevant to each business and for each environment. The knowledge base may also include standards for minimum program qualities and the level of documentation required for proof in answering the question which sets a standard used as a guide through the interviews with process owners." (See paragraph [0058]). The specification does not describe or suggest that any one person prioritizes risks. Rather, the description of risk prioritization is included within a description of multiple tasks undertaken by the server including, for example, prioritizing a list of compliance requirements. (See, for example, paragraph [0068].) Each task performed by the server is completed using the knowledge base, among other things. As such, Applicants submit that the priorization of risks by the server is described in the specification.

With regards to Claims 32, 33, 35, and 36, the Office Action asserts that the specification does not describe how the server is programmed to "assemble the cross-functional team and conduct an interview with a person...." Moreover, the Office Action asserts that "[o]ne of skill in the art would not be able to make the server do what is claimed and undue experimentation would be involve." Applicants respectfully traverse these assertions. Specifically, Applicants submit that the specification provides at paragraph [0056], for example, that "[t]he cross-functional team is assembled 72 using a knowledge base which is stored on server 12 and may include any information relevant to the assembly 72 of a cross-functional team." A server may be programmed by one of ordinary skill in the art to program the server to assemble a cross-functional team based on information contained in the knowledge base. Applicants submit that such a task is possible without undue experimentation.

With regards to Claim 34, the Office Action asserts that "one of skill in the art would not be able to go about and make a server that can create a questionnaire as claimed." Applicants respectfully traverse this assertion. Specifically, Applicants submit that the specification provides at paragraphs [0057-0060], for example, that a knowledge base is used to identify process owners and/or interviewees, determine what constitutes an affirmative answer to a question, and to conduct an interview. A server may be programmed by one of ordinary skill in the art to program the server to create a questionnaire based on information contained in the knowledge base. Applicants submit that such a task is described in the specification and is possible without undue experimentation.

With regards to Claims 39-42, the Office Action asserts that "[t]he server is not capable of knowing what the business management members know and cannot map a risk model, compile, compliance requirements and prioritize them, assign a severity rating (disclosed as being done by people), etc. One of skill in the art would not be able to go about and make a server that can create a questionnaire as claimed." Applicants respectfully traverse these assertions. Specifically, Applicants submit that one skilled in the art would be capable of programming the server to compile and prioritize a list of compliance requirements, construct a QFD, assign a severity rating for non-compliance with requirements, assess and evaluate compliance policies, map business risk models, and/or prioritize a severity level of each non-compliance based on information stored in the knowledge base. As such, Applicants submit that such tasks are described in the specification and are possible without undue experimentation.

With regards to Claims 43,-56, 58, and 60-62, the Office Action asserts that people are described as completing the recited tasks of listing compliance requirements, prioritizing risks, assigning severity ratings and process strengths, mapping a risk model, identifying possible failure modes, assigning occurrence and detection factors, and defining recommended actions. Applicants respectfully traverse these assertions and submit that one skilled in the art would be capable of programming a server to accomplish such tasks based on information stored in a knowledge base. As such, Applicants submit that such server-based tasks are described in the specification.

Accordingly, Applicants submit that the recitations of Claims 31-56, 58, and 60-62 are described in the specification such that one of ordinary skill in the art would not require undue experimentation.

Claim 75 has been canceled. Claims 63-74 recites a computer that is configured to perform steps substantially identical to those described with regards to Claims 31-36, 39-56, 58, and 60-62 above. As such, the recitations of Claim 63-74 are likewise submitted to be supported in the originally filed specification.

Claims 76-89 recites a computer program that includes at least one code segment for performing steps substantially identical to those described with regards to Claim 31-36, 39-56, 58, and 60-62 above. As such, the recitations of Claim 76-89 are likewise submitted to be supported in the originally filed specification.

For at least the reasons set forth above, Applicants submit that the specification meets the requirements of Section 112, first paragraph. Specifically, Applicants respectfully submit that the specification, including the figures, would enable one skilled in the art to make and/or use the invention as described in the present patent application. Accordingly, Applicants respectfully request that the Section 112, first paragraph, rejection of Claims 1-25, 27, 28, 30-56, 58, 60-89, and 119-122 be withdrawn.

The rejection of Claim 11 under 35 U.S.C. § 112, second paragraph, as being indefinite is respectfully traversed. Applicants have amended Claim 11 to recite "prioritizing compliance risk areas associated with the business' highest risks."

For at least the reasons set forth above, Applicants respectfully request that the Section 112, second paragraph, rejection of Claim 11 be withdrawn.

The rejection of Claims 1-16, 18-23, 25, 27, 28, 30-45, 47-53, 55, 56, 58, 60-89, and 119-122 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent Publication No. 2002/0120642 to Fetherston (hereinafter referred to as "Fetherston") in view of U.S. Patent 6,912,502 to Buddle, et al. (hereinafter referred to as "Buddle") is respectfully traversed.

Applicants respectfully submit that no combination of Fetherston and Buddle describes or suggests the claimed invention. At least one of the differences between Fetherston and Buddle and the present invention is that no combination of Fetherston and Buddle describes or suggests storing in the database compliance information including persons responsible for compliance within each functional area within the business.

Moreover, Applicants submit that no combination of Fetherston and Buddle describes or suggests calculating a risk prioritization number (RPN) for each compliance risk identified based on the data stored in the database, wherein the RPN represents a relative compliance risk of a particular failure mode including the severity rating, the occurrence rating, and the detection rating.

Fetherston describes a system for assisting an organization to implement and maintain compliance management programs. The system includes a plurality of modules relating to particular compliance obligations. Specifically, the system includes a master database containing information on the compliance obligations, a slave database containing information and activities (i.e., incidents or accidents) in the organization and assessments of the organization. More specifically, the master database includes input/output devices where a user may access a plurality of modules wherein each module is related to a particular piece of legislation, and the module is presented to the user on a display device. The display device also includes a plurality of sub-modules such as text documents that are stored in a storage unit and memory for display on a display unit when selected by the user. The user may select a sub-module that displays a risk assessment form permitting the user to enter and store data in the slave database about hazards in an organization about which the user has knowledge, such as an accident or a workplace ergonomics issue. The sub-module forces the user to follow a process and pattern of data entry into the various risk assessment forms. Once the data is entered by the user, the data is stored in the slave database. Fetherston also describes a risk assessment means that compares data in the slave database to compliance criteria from the master database. Specifically, the risk assessment means determines a numerical priority or risk assessment rating as the product of severity and frequency. A rating that exceeds a certain rating is brought to the attention of the user. Moreover, Fetherston describes that reports detailing particular hazards may be produced.

Buddle describes a method for compliance management in the financial services industry. First, a user identifies one or more business processes that may be subject to one or more regulations and/or constraints. Compliance requirements are then specified, and the user then specifies ownership of the requirements. The requirements are used to determine compliances risks and/or issues using, for example, risk propagation. One or more dashboards may be used to identify compliance issues, and to collect, process, and display data to enable identification of compliance issues. Next, an action plan is created for one or more compliance issues. Results of the action plan are tracked, reviewed, and/or analyzed to ensure that the action plans are being properly implemented.

Claim 1 recites a method for conducting a consistent, documented and yet repeatable compliance risk assessment and mitigation process, using a network-based system including a server system coupled to a centralized database and at least one client system. The method includes "*storing in the database compliance information including at least one questionnaire relating to compliance, compliance requirements for each functional area within a business, and persons responsible for compliance within each functional area within the business* . . . displaying a questionnaire on a client system associated with a person responsible for compliance with at least one functional area within the business, the questionnaire is transmitted from the server system to the client system of the compliance person and is generated using the compliance information stored within the database . . . receiving at the server a response inputted by the compliance person to the displayed questionnaire . . . processing the response to the displayed questionnaire at the server . . . prioritizing compliance risks for the business including identifying compliance risks for each functional area within the business, and prioritizing the compliance risks from high to low based on a severity rating of non-compliance . . . identifying, for each compliance risk identified, potential compliance failure modes, potential causes and effects of such compliance failure modes, current controls in place, an occurrence rating, and a detection rating, wherein the occurrence rating is a value representing a likelihood of occurrence of the potential compliance failure modes and the detection rating is a value representing whether current controls in place will detect potential compliance failure modes . . . storing the risks, the risk priority, the failure modes, the causes and effects of the failure modes, the current controls in place, the occurrence ratings, and the detection ratings in the database . . . *calculating a risk prioritization number (RPN) for each compliance risk identified based on the data stored in the database, wherein the RPN represents a relative compliance risk of a particular failure mode and is a product of the severity rating, the occurrence rating, and the detection rating* . . . implementing risk monitoring and control mechanisms to mitigate compliance risks based on the calculated RPNs including recommending actions to be implemented to reduce the calculated RPNs . . . creating at least one policy dashboard summarizing actions to be taken based on the recommended actions and key metrics for monitoring the implementation of the actions." (Emphasis added)

Neither Fetherston nor Buddle, considered alone or in combination, describes or suggests a method as recited in Claim 1. More specifically, neither Fetherston nor Buddle, considered alone or in combination, describes or suggests a method for conducting a compliance risk assessment and mitigation process that includes calculating a risk prioritization number (RPN) for each compliance risk identified based on the data stored in the database, wherein the RPN represents a relative compliance risk of a particular failure mode and is a product of the severity rating, the occurrence rating, and the detection rating, and wherein the severity rating is a value representing a severity of occurrence of the potential failure modes, the occurrence rating is a value representing a likelihood of occurrence of the potential compliance failure modes, and the detection rating is a value representing whether current controls in place will detect potential compliance failure modes. Moreover, neither Fetherston nor Buddle, considered alone or in combination, describes or suggests storing in the database compliance information including persons responsible for compliance within each functional area within the business.

Rather, Fetherston describes a system for assisting an organization to implement and maintain compliance management programs. The system includes a master database containing information on the compliance obligations, a slave database containing information and activities, such as incidents or accidents in the organization, and assessments of the organization. The system allows any user to input information into the slave database, such as knowledge of improper operating conditions and/or improper ergonomic working conditions. Buddle describes a method for financial service compliance management including using dashboards to collect, process, and display data to enable identification of compliance risks and to collect dynamic data for analysis.

The Office Action asserts at page 9 that "[i]dentifying the department also identifies the persons responsible for compliance (i.e., the employees in that department)." Fetherston fails to teach the step of storing compliance information including a plurality of process owners responsible for compliance within each functional area within the business. The "Department" data entry field referred to in the Office Action is described by Fetherston in paragraph [0056]. Specifically, Fetherston describes that "[a]ll staff in each department are identified and this information is made available to the user *so that the user may select the staff member who has had an accident* and place all relevant information about that staff member in the slave database as a record of the accident *even if that person is not part of the department*." As such, Applicants submit that Fetherston does not describe or suggest storing compliance information including a plurality of process owners responsible for compliance within each functional area within the business.

Accordingly, for at least the reasons set forth above, Claim 1 is submitted to be patentable over Fetherston in view of Buddle.

Claims 2-16, 18-23, 25, 27, 28, 30, and 119 depend from independent Claim 1. When the recitations of Claims 2-16, 18-23, 25, 27, 28, 30, and 119 are considered in combination with the recitations of Claim 1, Applicants submit that dependent Claims 2-16, 18-23, 25, 27, 28, 30, and 119 likewise are patentable over Fetherston in view of Buddle.

Claim 31 recites system for identifying and quantifying compliance. The system includes "at least one computer . . . *a database for storing compliance information including at least one questionnaire relating to compliance, compliance requirements for each functional area within a business, and persons responsible for compliance within each functional area within the business* . . . a server . . . a network connecting said computer to said server, wherein said server configured to display a questionnaire on said computer associated with a person responsible for compliance with at least one functional area within the business, said network is configured to transmit the questionnaire from said server to said computer of the compliance person and is generated using the compliance information stored within the database, said server is configured to: receive a response inputted by the compliance person to the displayed questionnaire . . . process the response to the displayed questionnaire . . . prioritize compliance risks for the business including identifying compliance risks for each functional area within the business, and prioritizing the compliance risks from high to low based on a severity rating of non-compliance . . . identify, for each compliance risk identified, potential compliance failure modes, potential causes and effects of such compliance failure modes, current controls in place, an occurrence rating, and a detection rating, wherein the occurrence rating is a value representing a likelihood of occurrence of the potential compliance failure modes and the detection rating is a value representing whether current controls in place will detect potential compliance failure modes . . . store the risks, the risk priority, the failure modes, the causes and effects of the failure modes, the current controls in place, the occurrence rating, and the detection ratings in the database . . . *calculate a risk prioritization number (RPN) for each compliance risk identified based on the data stored in the database, wherein the RPN represents a relative compliance risk of a particular failure mode and is a product of the severity rating, the occurrence rating, and the detection rating* . . . recommend risk monitoring and control mechanisms to mitigate compliance risks based on the calculated RPNs including recommending actions to be implemented to reduce the calculated RPNs . . . create at least one policy dashboard summarizing actions to be taken based on the recommended actions and key metrics for monitoring the implementation of the actions."

Claim 31, as amended herein, recites a system for identifying and quantifying compliance that includes a server configured to perform steps essentially similar to those recited in Claim 1. Thus, Applicants submit that Claim 31 is submitted to be patentable over Fetherston in view of Buddle for reasons that correspond to those given with respect to Claim 1.

Claims 32-45, 47-53, 55, 56, 58, 60-62, and 120 depend from independent Claim 31. When the recitations of Claims 32-45, 47-53, 55, 56, 58, 60-62, and 120 are considered in combination with the recitations of Claim 31, Applicants submit that dependent Claims 32-45, 47-53, 55, 56, 58, 60-62, and 120 likewise are patentable over Fetherston in view of Buddle.

Claim 63 recites computer programmed to "*store in a database compliance information including at least one questionnaire relating to compliance, compliance requirements for each functional area within a business, and persons responsible for compliance within each functional area within the business* . . . display a questionnaire for a person responsible for compliance with at least one functional area within the business, the questionnaire is generated using the compliance information stored within the database . . . receive a response inputted by the compliance person to the displayed questionnaire . . . process the response to the displayed questionnaire . . . prioritize compliance risks for the business including identifying compliance risks for each functional area within the business, and prioritizing the compliance risks from high to low based on a severity rating of non-compliance . . . identify, for each compliance risk identified, potential compliance failure modes, potential causes and effects of such compliance failure modes, current controls in place, an occurrence rating, and a detection rating, wherein the occurrence rating is a value representing a likelihood of occurrence of the potential compliance failure modes the detection rating is a value representing whether current controls in place will detect potential compliance failure modes . . . store the risks, the risk priority, the failure modes, the causes and effects of the failure modes, the current controls in place, the occurrence ratings, and the detection ratings in the database . . . *calculate a risk prioritization number (RPN) for each compliance risk identified based on the data stored in the database, wherein the RPN represents a relative compliance risk of a particular failure mode and is a product of the severity rating, the occurrence rating, and the detection rating* . . . recommend risk monitoring and control mechanisms to mitigate compliance risks based on the calculated RPNs including recommending actions to be implemented to reduce the calculated RPNs . . . create at least one policy dashboard summarizing actions to be taken based on the recommended actions and key metrics for monitoring the implementation of the actions."

Claim 63, as amended herein, recites a system for identifying and quantifying compliance that includes a server configured to perform steps essentially similar to those recited in Claim 1. Thus, Applicants submit that Claim 63 is submitted to be patentable over Fetherston in view of Buddle for reasons that correspond to those given with respect to Claim 1.

Claim 75 has been canceled. Claims 64-74 and 121 depend from independent Claim 63. When the recitations of Claims 64-74 and 121 are considered in combination with the recitations of Claim 63, Applicants submit that dependent Claims 64-74 and 121 likewise are patentable over Fetherston in view of Buddle.

Claim 76 recites a computer program embodied on a computer readable medium for managing compliance risk assessment to enable businesses to develop broader and deeper coverage of compliance risks, using a network based system including a server system coupled to a centralized database and at least one client system. The computer program includes a code segment that "*stores in the database compliance information including at least one questionnaire relating to compliance, compliance requirements for each functional area within a business, and persons responsible for compliance within each functional area within the business* . . . displays a questionnaire on a client system associated with a person responsible for compliance with at least one functional area within the business, the questionnaire is transmitted from the server system to the client system of the compliance person and is generated using the compliance information stored within the database . . .

receives a response inputted by the compliance person to the displayed questionnaire . . . processes the response to the displayed questionnaire at the server . . . prioritizes compliance risks for the business including identifying compliance risks for each functional area within the business, and prioritizing the compliance risks from high to low based on a severity rating of non-compliance . . . identifies, for each compliance risk identified, potential compliance failure modes, potential causes and effects of such compliance failure modes, current controls in place, an occurrence rating, and a detection rating, wherein the occurrence rating is a value representing a likelihood of the potential compliance failure modes and the detection rating is a value representing whether current controls in place will detect potential compliance failure modes . . . stores the risks, the risk priority, the failure modes, the causes and effects of the failure modes, the current controls in place, occurrence ratings, and detection ratings in the database . . . *calculates a risk prioritization number (RPN) for each compliance risk identified based on the data stored in the database, wherein the RPN represents a relative compliance risk of a particular failure mode and is a product of the severity rating, the occurrence rating, and the detection rating* . . . recommends risk monitoring and control mechanisms to mitigate compliance risks based on the calculated RPNs including recommending actions to be implemented to reduce the calculated RPNs . . . creates at least one policy dashboard summarizing actions to be taken based on the recommended actions and key metrics for monitoring the implementation of the actions."

Claim 76, as amended herein, recites a system for identifying and quantifying compliance that includes a server configured to perform steps essentially similar to those recited in Claim 1. Thus, Applicants submit that Claim 76 is submitted to be patentable over Fetherston in view of Buddle for reasons that correspond to those given with respect to Claim 1.

Claims 77-89 and 122 depend from independent Claim 76. When the recitations of Claims 77-89 and 122 are considered in combination with the recitations of Claim 76, Applicants submit that dependent Claims 77-89 and 122 likewise are patentable over Fetherston in view of Buddle.

Applicants submit that dependent Claims 77-89 and 122 likewise are patentable over Fetherston in view of Buddle.

For at least the reasons set forth above, Applicants respectfully request that the Section 103 rejection of Claims 1-16, 18-23, 25, 27, 28, 30-45, 47-53, 55, 56, 58, 60-89, and 119-122 be withdrawn.

In view of the foregoing amendment and remarks, all the claims now active in this application are believed to be in condition for allowance. Reconsideration and favorable action is respectfully solicited.

Respectfully submitted,

Daniel M. Fitzgerald
Registration No. 38,880
ARMSTRONG TEASDALE LLP
One Metropolitan Square, Suite 2600
St. Louis, Missouri 63102-2740
(314) 621-5070